

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10017334-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Richard Paul TARQUINI et al.

Confirmation No.: 4709

Application No.: 10/003820

Examiner: Alomari Firas B.

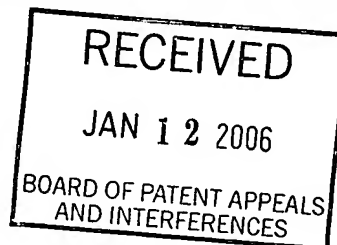
Filing Date: October 31, 2001

Group Art Unit: 2136

Title: **NODE, METHOD AND COMPUTER READABLE MEDIUM FOR OPTIMIZING PERFORMANCE OF SIGNATURE
RULE MATCHING IN A NETWORK**

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF



Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on Nov. 15, 2005

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) \$500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

RECEIVED
JAN 17 2006
Technology Center 2100

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month
\$120

☐ 2nd Month
\$450

☐ 3rd Month
\$1020

☐ 4th Month
\$1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of \$ 500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit: January 9, 2006

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile:

Typed Name: Cindy C. Dioso

Signature: Cindy C. Dioso

Respectfully submitted,

Richard Paul TARQUINI et al.

By: James L. Baudino

James L. Baudino

Attorney/Agent for Applicant(s)

Reg No. : 43,486

Date : January 9, 2006

Telephone : (214) 855-7544

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**APPEAL FROM THE EXAMINER TO THE BOARD
OF PATENT APPEALS AND INTERFERENCES**

In re Application of: Richard Paul Tarquini et al.
Serial No.: 10/003,820
Filing Date: 10/31/2001
Group Art Unit: 2136
Examiner: Alomari Firas B.
Title: NODE, METHOD AND COMPUTER READABLE
MEDIUM FOR OPTIMIZING PERFORMANCE OF
SIGNATURE RULE MATCHING IN A NETWORK
Docket No.: 10017334-1

MAIL STOP: APPEAL BRIEF PATENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

APPEAL BRIEF

Applicants has appealed to the Board of Patent Appeals and Interferences from the decision of the Examiner mailed September 15, 2005, finally rejecting Claims 1-17. Applicants filed a Notice of Appeal on November 15, 2005. Applicants respectfully submit herewith this Appeal Brief with authorization to charge the statutory fee of \$500.00.

REAL PARTY IN INTEREST

The present application was assigned to Hewlett-Packard Company as indicated by an assignment from the inventor recorded on March 18, 2002 in the Assignment Records of the United States Patent and Trademark Office at Reel 012705, Frame 0880. The present application was subsequently assigned to Hewlett-Packard Development Company, L.P. as indicated by an assignment from Hewlett-Packard Company recorded on September 30, 2003 in the Assignment Records of the United States Patent and Trademark Office at Reel 014061, Frame 0492.

RELATED APPEALS AND INTERFERENCES

There are no known appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

STATUS OF CLAIMS

Claims 1-17 stand rejected pursuant to a Final Office Action mailed September 15, 2005. Claims 1-17 are presented for appeal.

STATUS OF AMENDMENTS

No amendment has been filed subsequent to the mailing of the Final Office Action.

SUMMARY OF CLAIMED SUBJECT MATTER

Embodiments of the present invention as defined by independent Claim 1 are directed toward a node (85) of a network (100) for managing an intrusion protection system, the node (85) comprising a memory module (274) for storing data in machine-readable format for retrieval and execution by a central processing unit (272) and an operating system (275) comprising a network stack (90) comprising a protocol driver (135) and a media access control driver (145) and operable to execute an intrusion protection system management application (279), the management application (279) operable to receive text-file (277A-277N) input from an input device (281), the text-file

(277A-277N) defining a network-exploit rule and comprising at least one field. (at least at page 11, lines 25-31; page 12, lines 1-4; page 13, lines 8-31; page 15, lines 12-31; page 16, lines 1-13 and 22-31; page 17, lines 1-24; page 18, lines 7-25, page 19, lines 1-7; and figures 2, 3 and 5).

Embodiments of the present invention as defined by independent Claim 8 are directed toward a method of distributing command and security updates in a network (100) having an intrusion protection system (91) comprising generating a text-file (277A-277N) defining a network-exploit rule and specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file (277A-277N). (at least at page 11, lines 25-31; page 12, lines 1-4; page 13, lines 8-31; page 15, lines 12-31; page 16, lines 1-13 and 22-31; page 17, lines 1-24; page 18, lines 7-25, page 19, lines 1-31; page 20, lines 1-27; and figures 2, 3 and 5).

Embodiments of the present invention as defined by independent Claim 13 are directed toward a computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor (272), cause the processor (272) to perform a computer method of reading input from an input device (281) of the computer, compiling the input into a machine-readable signature file (281A-281N) comprising machine-readable logic representative of the network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field, evaluating the machine-readable signature file (281A-281N), and determining the value of the at least one field of the machine-readable signature file (281A-281N). (at least at page 11, lines 25-31; page 12, lines 1-4; page 13, lines 8-31; page 15, lines 12-31; page 16, lines 1-13 and 22-31; page 17, lines 1-24; page 18, lines 7-25, page 19, lines 1-31; page 20, lines 1-27; and figures 2, 3 and 5).

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-17 are rejected under 35 U.S.C. §103(a) as being unpatentable in view of U.S. Patent No. 6,279,113 issued to Vaidya (hereinafter “*Vaidya*”) in view of U.S. Patent No. 6,134,664 issued to Walker (hereinafter “*Walker*”).

ARGUMENT

A. Standard

1. 35 U.S.C. § 103

To establish a *prima facie* case of obviousness under 35 U.S.C. § 103, three basic criteria must be met: First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; second, there must be a reasonable expectation of success; and finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Vaeck*, 947 F.2d 488, (Fed. Cir. 1991); M.P.E.P. § 2143. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant’s disclosure. *Id.* Further, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990); M.P.E.P. § 2143.01. Additionally, not only must there be a suggestion to combine the functional or operational aspects of the combined references, but also the prior art is required to suggest both the combination of elements and the structure resulting from the combination. *Stiftung v. Renishw PLC*, 945 F.2d 1173, 1183 (Fed. Cir. 1991). Moreover, where there is no apparent disadvantage present in a particular prior art reference, then generally there can be no motivation to combine the teaching of another reference with the particular prior art reference. *Winner Int’l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 (Fed. Cir. 2000).

B. Argument

1. First Ground of Rejection (Claims 1-7)

Claims 1-7 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Vaidya* in view of *Walker*. Of the rejected claims, Claim 1 is independent. Applicants respectfully submit that independent Claim 1 is patentable over the cited references and, therefore, Claims 2-7 are also patentable.

Embodiments of the present invention generally involve a node (85) of a network (100) for managing an intrusion prevention system (91) where the node (85) comprises an operating system (275) having a network stack (90) and operable to execute an intrusion protection management application (85) (at least at page 19, lines 8-31; and figure 5). In some embodiments of Applicants' invention, the management application (85) is configured to receive a text-file (277A-277N) via an input device (281) (e.g., a keyboard) (at least at page 15, lines 12-31; and figure 5). In such embodiments of the present invention, the text-file (277A-277N) comprises a text-based network-based exploit rule and comprises a logical description of an attack signature and a directive to execute upon the determination of a network intrusion (at least at page 15, lines 25-31). The text-file (277A-277N) is compiled into a machine-readable signature file (281A-281N) which may be transmitted to one or more nodes on the network (100) (at least at page 15, lines 25-31; page 16, lines 1-13; and figure 5). Further, in some embodiments, particular fields of the text-file (277A-277N) are used to designate a particular action or policy associated with a particular signature (281A-281N) (e.g., specifying a particular value in an enable/disable field of the text-file (277A-277N) enables/disables enforcement of intrusion prevention associated with the particular signature (281A-281N) (at least at page 17, lines 8-24). Accordingly, Claim 1 is directed toward a node of a network for managing an intrusion protection system and reciting "a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit" and "an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application, the management application operable to

receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field.”

In rejecting independent Claim 1, the Examiner has not provided sufficient reasoning or made any assertions as to why the Examiner believes that the portions of at least *Vaidya* referred to by the Examiner disclose particular limitations of Claim 1. The Examiner merely recites Applicants’ claim limitation(s) followed by a general recitation of column and line numbers of *Vaidya*, leaving Applicants guessing as to the Examiner’s intended meaning. For example, with respect to Applicants’ Claim 1 recitation of “an intrusion protection system management application” and “the management application operable to receive text-file input from an input device,” the Examiner merely states “(Col 6, Lines 11-18 and Col 7, Lines 12-24)” and “(Col 7, lines 24-36, and Col 6, Lines 53-56)” (Final Office Action, page 4) without indicating which components of *Vaidya* the Examiner is relying on to purportedly teach, for example, “an intrusion protection system management application,” “text-file input” or “an input device” as recited by Claim 1. Accordingly, for at least this reason, Applicants respectfully submit that the Examiner has not established a *prima facie* case of obviousness.

Regardless of the foregoing, Applicants submit that *Vaidya* does not disclose or even suggest the limitations of independent Claim 1 as asserted by the Examiner. For example, independent Claim 1 recites “an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application” where “the management application [is] operable to receive text-file input from an input device.” The portions of *Vaidya* referred to by the Examiner fail to disclose or even suggest at least these limitation(s) recited by independent Claim 1, and Applicants are unable to determine why the Examiner believes that the portions of *Vaidya* referred to by the Examiner purportedly teach at least these limitation(s). Applicants respectfully submit that such details are lacking in *Vaidya*, and the Final Office Action fails to explain why the Examiner believes that such details are present in *Vaidya*. As just one example,

Applicants submit that *Vaidya* does not teach or even suggest a “management application operable to receive text-file input from an input device” where the “text-file defin[es] a network-exploit rule” as recited by Claim 1 (emphasis added). In the Final Office Action, the Examiner refers to column 7, lines 24-36, and column 6, lines 53-56, of *Vaidya* as purportedly disclosing the above-referenced limitations of Claim 1 (Final Office Action, page 4). Applicants respectfully disagree. The portions of *Vaidya* referred to by the Examiner appear to be limited to disclosing a “signature profile.” Neither the portions of *Vaidya* referred to by the Examiner nor elsewhere in *Vaidya* disclose or even suggest that such “signature profile” of *Vaidya* is a “text-file,” much less that such signature profile of *Vaidya* is “receive[d] . . . from an input device” as recited by Claim 1. In fact, as discussed above, the Examiner does not explicitly identify any element of *Vaidya* the Examiner considers to correspond to the “input device” recited by Claim 1. Therefore, for at least these reasons also, Applicants submit that Claim 1 is patentable over the cited references.

Moreover, Applicants respectfully submit that there is no motivation or suggestion for combining reference teachings as proposed by the Examiner. For example, independent Claim 1 recites “the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field.” The Examiner admits that *Vaidya* does not disclose a text-file input comprising at least one field (Final Office Action, page 4), but the Examiner states that *Walker* discloses such limitation and that it would have been obvious to modify *Vaidya* to use signature files comprising at least one field (Final Office Action, pages 4 and 5). Applicants respectfully disagree.

Walker appears to be directed toward a system for reducing the volume of audit data that is to be evaluated by an intrusion detection system (*Walker*, Abstract, column 4, lines 37-40). *Walker* appears to indicate that such audit data, in the form of an audit trail record, for example, “comprises a plurality of fields” (*Walker*, column 11, lines 29-35). Based on the foregoing, the Examiner appears to arbitrarily import such “field” into a

signature file (“it would [have] been obvious . . . to modify [the] *Vaidya* system to use signature files comprising at least one field [sic]”) (Final Office Action, page 5). Applicants respectfully disagree. The “field” referred to by *Walker* is in an audit trail record and not part of a signature file. Accordingly, neither *Walker* nor *Vaidya*, alone or in combination, suggests including such “field” in a signature file as proposed by the Examiner. Moreover, the Examiner’s basis for including such “field” in a signature file appears to stem from the fact that an audit trail record as disclosed by *Walker* includes a “field,” and nothing more. However, *Vaidya* does not appear to disclose or even suggest that any data analyzed by the *Vaidya* system contains any such “fields” that would require that a signature file compared therewith would also require a similar “field,” nor has the Examiner explicitly identified any such disclosure or suggestion in *Vaidya*. To the contrary, the audit records containing the “field” appear to be limited to the *Walker* reference. Moreover, in support of the Examiner’s reasoning for combining reference teachings, the Examiner states:

One would be motivated to do so in order to enable the system to identify different signatures and take different set[s] of actions for the different signatures to improve the performance of the intrusion detection system.

(Final Office Action, page 5). Applicants respectfully disagree. The Examiner’s reasoning for including a “field” in a signature file appears to stem from the fact that *Walker* discloses a “field” in an audit record trail. However, the Examiner’s use of such modification as indicated above appears to be independent of whether the data to be compared against such signature field has a “field.” To the contrary, the Examiner’s proposed combination appears to require at least two different steps, neither of which are disclosed or even suggested by the cited references: 1) modifying a signature with a “field” apparently based on the fact that data to be compared with such signature includes a “field;” but 2) using such “field” in the signature file for purposes of identifying different signatures, which appears to be completely independent of whether the data packet in *Vaidya* to be compared against a signature file contains a “field.” Clearly, the Examiner’s bases for combining the reference teachings is unsupported and the Examiner

is using hindsight reasoning to piece together the teachings of the cited references to arrive at Applicants' claimed invention, which is improper. Therefore, for at least this reason also, the rejection of independent Claim 1 is improper and should be withdrawn.

In response to Applicants' response filed June 22, 2005, the Examiner appears to refer to various websites to purportedly teach that a string of characters in the payload of a network message indicates that the message contains malicious content, and the Examiner appears to equate such purported teaching to the "present invention's text file defining a [sic] network exploit rule" (Final Office Action, page 2). Applicants respectfully disagree. First, the Examiner appears to be referring to "the payload of a network message." Instead, Applicants' Claim 1 recites "text-file input . . . defining a network-exploit rule" (emphasis added). Second, the Examiner appears to automatically equate a "string of characters" as a text-file without any apparent basis for doing so. For example, Applicants respectfully submit that the character string "#@6()*\$%d6" is not a text-based attack signature description defining a network-exploit rule. Accordingly, for at least this reason also, Applicants respectfully submit that Claim 1 is patentable over the cited references.

Accordingly, for at least the reasons discussed above, Applicants respectfully submit that independent Claim 1 is clearly patentable over the cited references and, therefore, Applicants respectfully request that Claim 1, and Claims 2-7 that depend therefrom, be allowed.

2. Claims 8-12

Claims 8-12 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Vaidya* in view of *Walker*. Of the rejected claims, Claim 8 is independent. Applicants respectfully submit that independent Claim 8 is patentable over the cited references and, therefore, Claims 9-12 are also patentable.

Independent Claim 8 is directed toward a method of distributing command and security updates in a network having an intrusion protection system and recites “generating a text-file defining a network-exploit rule” and “specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file.” At least for the reasons discussed above in connection with independent Claim 1, Applicants respectfully submit that the rejection of Claim 8 is improper and should be withdrawn. For example, the Examiner has not provided sufficient reasoning or made any assertions as to why he believes that the portions of at least *Vaidya* referred to by the Examiner disclose particular limitations of Claim 8. As noted previously, the Examiner merely recites Applicants’ claim limitation(s) followed by a general recitation of column and line numbers of *Vaidya*. For example, with respect to Applicants’ Claim 8 recitation of “generating a text-file defining a network-exploit rule,” the Examiner merely states “(Col 5, Lines 33-39; Col 5, Lines 51-63 and Col 6, Lines 44-56)” (Final Office Action, page 8) without indicating which components of *Vaidya* the Examiner is relying on to purportedly teach, for example, “generating a text-file” or a text-file that “defin[es] a network-exploit rule” as recited by Claim 8. To the contrary, Applicants respectfully submit that *Vaidya* does not disclose or even suggest such limitation(s). Further *Walker* does not appear to remedy at least this deficiency of *Vaidya*, nor did the Examiner rely on *Walker* to remedy at least this deficiency of *Vaidya*. Accordingly, for at least this reason, Applicants respectfully submit that the rejection of Claim 8 is improper.

Additionally, Claim 8 recites “specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file.” The Examiner admits that *Vaidya* does not disclose these limitations (Final Office Action, page 8), but the Examiner states that *Walker* teaches such limitation and that it would have been obvious to modify *Vaidya* to use signature files comprising at least one field (Final Office Action, page 8). Applicants respectfully disagree. As discussed above in connection with independent Claim 1, Applicants submit that there is no motivation or suggestion to combine reference teachings as suggested by

the Examiner based solely on an audit trail record having a “field” (as disclosed by *Walker*). For example, the “field” referred to by *Walker* is in an audit trail record and not part of a signature file. Accordingly, neither *Walker* nor *Vaidya*, alone or in combination, suggests including such “field” in a signature file as proposed by the Examiner. Moreover, the Examiner’s basis for including such “field” in a signature file appears to stem from the fact that an audit trail record as disclosed by *Walker* includes a “field,” and nothing more. However, *Vaidya* does not appear to disclose or even suggest that any data analyzed by the *Vaidya* system contains any such “fields” that would require that a signature file compared therewith would also require a similar “field,” nor has the Examiner explicitly identified any such disclosure or suggestion in *Vaidya*.

Additionally, neither *Vaidya* nor *Walker* disclose or even suggest “a text-file defining a network exploit rule” as recited by Claim 8 (emphasis added). As discussed above in connection with independent Claim 1, a “character string” in a network message as referred to by the Examiner is not a text-based attack signature description defining a network-exploit rule. Therefore, for at least this reason also, Claim 8 is patentable over the cited references.

Further, the Examiner appears to completely ignore various limitations of Claim 8. For example, *Walker* does not appear to disclose or even suggest “specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file” as recited by Claim 8 (emphasis added), nor has the Examiner explicitly identified any such disclosure in either *Vaidya* or *Walker*. In fact, the Examiner does not even refer to these limitations in the Examiner’s reference to *Walker* (see the Final Office Action, page 8). Accordingly, for at least this reason also, Claim 8 is patentable over the cited references.

Accordingly, for at least the reasons discussed above, Applicants respectfully submit that independent Claim 8 is clearly patentable over the cited references and,

therefore, Applicants respectfully request that Claim 8, and Claims 9-12 that depend therefrom, be allowed.

3. Claims 13-17

Claims 13-17 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Vaidya* in view of *Walker*. Of the rejected claims, Claim 13 is independent. Applicants respectfully submit that independent Claim 13 is patentable over the cited references and, therefore, Claims 14-17 are also patentable.

Independent Claim 13 recites “reading input from an input device of the computer,” “compiling the input into a machine-readable signature file comprising machine-readable logic representative of the network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field,” “evaluating the machine-readable signature file” and “determining the value of the at least one field of the machine-readable signature file.” For at least the reasons discussed above in connection with independent Claim 1 and 8, Applicants respectfully submit that the rejection of Claim 13 is improper. For example, as stated above, the Examiner merely refers generally to various portions of *Vaidya* as purportedly teaching the limitations of Claim 13 without indicating which components of *Vaidya* the Examiner is relying on to purportedly teach such limitations. Further, even when Applicants assume which components of *Vaidya* the Examiner may be referring to as purportedly teaching the limitations of Claim 13, the portions of *Vaidya* referenced by the Examiner are insufficient. For example, the Examiner refers to column 5, lines 51-63, of *Vaidya* as teaching “reading input from an input device of the computer” and “compiling the input into a machine-readable signature file” as recited by Claim 13. Applicants respectfully disagree. Column 5, lines 51-63, of *Vaidya* recite the following:

A configuration generator 28 is connected to the database handler to enable the network administrator to define the configuration of network objects on the LAN 11 and the remote network 24. The configuration generator 28 also enables the administrator to define the connection of both

the LAN 11 and the remote network 24 to the Internet. Network objects include devices such as . . . [and] further include applications and files stored in memory within those devices. Based on the network configuration data generated by the configuration generator 28, the database handler 26 assigns sets of attack signatures profiles to each data collector 10.

Thus, the portion referred to by the Examiner appears to disclose that for a particular network object of *Vaidya*, a particular set of signature profiles will be used to analyze data packets directed to that particular network object (see also column 6, lines 1-15, of *Vaidya*). Accordingly, *Vaidya* does not disclose or even suggest, in the portion referred to by the Examiner or elsewhere in *Vaidya*, “reading input from an input device of the computer” and “compiling the input into a machine-readable signature file” as recited by Claim 13. Moreover, *Walker* does not appear to remedy at least these deficiencies of *Vaidya*, nor did the Examiner rely on *Walker* to remedy at least this deficiency of *Vaidya*.

Further, as discussed above, Applicants submit that there is no motivation or suggestion to combine reference teachings as suggested by the Examiner based solely on an audit trail “field” as suggested by the Examiner. For example, the “field” referred to by *Walker* is in an audit trail record and not part of a signature file. Accordingly, neither *Walker* nor *Vaidya*, alone or in combination, suggests including such “field” in a signature file as proposed by the Examiner. Moreover, the Examiner’s basis for including such “field” in a signature file appears to stem from the fact that an audit trail record as disclosed by *Walker* includes a “field,” and nothing more. However, *Vaidya* does not appear to disclose or even suggest that any data analyzed by the *Vaidya* system contains any such “fields” that would require that a signature file compared therewith would also require a similar “field,” nor has the Examiner explicitly identified any such disclosure or suggestion in *Vaidya*. Clearly, the Examiner’s bases for combining the reference teachings is unsupported and the Examiner is using hindsight reasoning to piece together the teachings of the cited references to arrive at Applicants’ claimed invention, which is improper. Therefore, for at least this reason also, the rejection of independent Claim 13 is improper.

Additionally, Claim 13 recites “a machine-readable signature file comprising machine-readable logic representative of the network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field” (emphasis added). The Examiner appears to ignore at least these limitation(s) because the Examiner does not appear to even refer to these limitation(s) in the Examiner’s reference to Claim 13 and/or *Walker* (see the Final Office Action, page 9). Accordingly, for at least these reasons, the rejection of Claim 13 is improper.

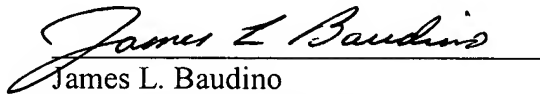
Accordingly, for at least the reasons discussed above, independent Claim 13 is clearly patentable over the cited references. Therefore, Claim 13, and Claims 14-17 that depend therefrom, are in condition for allowance.

CONCLUSION

Applicants have demonstrated that the present invention as claimed is clearly distinguishable over the art cited of record. Therefore, Applicants respectfully request the Board of Patent Appeals and Interferences to reverse the final rejection of the Examiner and instruct the Examiner to issue a notice of allowance of all claims.

The Commissioner is authorized to charge the statutory fee of \$500.00 to Deposit Account No. 08-2025 of Hewlett-Packard Company. Although no other fee is believed due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,


James L. Baudino
Registration No. 43,486

Date: January 9, 2006

Correspondence To:

L. Joy Griebenow
Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400
Tel. (970) 898-3884

CLAIMS APPENDIX

1. A node of a network for managing an intrusion protection system, the node comprising:
 - a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit; and
 - an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application, the management application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field.
2. The node according to claim 1, wherein the network exploit rule further comprises a field selected from the group consisting of an ENABLED field and a SEVERITY field.
3. The node according to claim 1, wherein the node is operable to compile the text-file into a machine-readable signature-file and transmit the machine-readable signature-file to at least one other node of the network.
4. The node according to claim 1, further comprising a database, the node operable to store a plurality of text-files, each respectively defining a network-exploit rule, in the database.
5. The node according to claim 2, further comprising a machine-readable signature-file database operable to store a plurality of machine-readable signature-files each generated from one of a respective plurality of text-files, the management application operable to transmit a subset of the plurality of machine-readable signature-files to another node connected to the network.
6. The node according to claim 5, wherein the subset comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value.

7. The node according to claim 5, wherein the management application is operable to accept a SEVERITY threshold from the input device and the subset comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than the threshold.

8. A method of distributing command and security updates in a network having an intrusion protection system, comprising:
generating a text-file defining a network-exploit rule; and
specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file.

9. The method according to claim 8, further comprising storing a plurality of text-files in a database, each text-file defining a network-exploit rule.

10. The method according to claim 9, further comprising transmitting, by a management node of the network, a subset of the plurality of machine-readable signature-files to a node in the network.

11. The method according to claim 10, wherein the subset of machine-readable signature-files comprises all of the plurality of machine-readable signature-files each generated from a respective one of the plurality of text-files that has the respective ENABLED field asserted.

12. The method according to claim 10, further comprising specifying a priority level threshold, the subset of the plurality of machine-readable signature-files comprised of all machine-readable signature-files generated from a respective one of the plurality of text-files having a SEVERITY level field value equal to or greater than the threshold.

13. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

reading input from an input device of the computer;

compiling the input into a machine-readable signature file comprising machine-readable logic representative of the network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field;

evaluating the machine-readable signature file; and

determining the value of the at least one field of the machine-readable signature file.

14. The computer readable medium according to claim 13, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of specifying a SEVERITY threshold value.

15. The computer readable medium according to claim 14, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of transmitting the machine-readable signature file to another node of the network upon determining the value of the SEVERITY field is greater than the threshold.

16. The computer readable medium according to claim 13, further comprising a set of instruction that, when executed by the processor, cause the processor to perform the computer method of generating a text-file from the input, the text-file specifying the network-exploit rule and the at least one field, the machine-readable signature file compiled from the text file.

17. The computer readable medium according to claim 13, further comprising a set of instruction that, when executed by the processor, cause the processor to perform the computer method of transmitting the machine-readable signature file to another node of the network upon determining the ENABLED field value is logically asserted.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None